

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 4 年    2 月 1 2 日  
Date of Application:

出 願 番 号                      特 願 2 0 0 4 - 0 3 5 4 8 1  
Application Number:

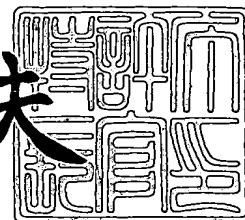
[ST. 10/C] :                      [ J P 2 0 0 4 - 0 3 5 4 8 1 ]

出      願      人                      富 士 ゼ ロ ッ ク ス 株 式 会 社  
Applicant(s):

2 0 0 4 年    3 月 2 4 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号    出証特 2 0 0 4 - 3 0 2 4 3 0 5

【書類名】 特許願  
【整理番号】 FE04-00132  
【提出日】 平成16年 2月12日  
【あて先】 特許庁長官殿  
【国際特許分類】 H04L 12/46 100  
【発明者】  
    【住所又は居所】 東京都港区赤坂二丁目 1 7 番 2 2 号 富士ゼロックス株式会社内  
    【氏名】 吉田 武央  
【特許出願人】  
    【識別番号】 000005496  
    【氏名又は名称】 富士ゼロックス株式会社  
【代理人】  
    【識別番号】 110000154  
    【氏名又は名称】 特許業務法人はるか国際特許事務所  
    【代表者】 金山 敏彦  
    【電話番号】 03-5367-2790  
【先の出願に基づく優先権主張】  
    【出願番号】 特願2003- 59162  
    【出願日】 平成15年 3月 5日  
【手数料の表示】  
    【予納台帳番号】 185835  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 0301849

**【書類名】 特許請求の範囲****【請求項 1】**

クライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムであって、

前記認証用サーバは、

前記接続サーバにおいて利用される第 1 接続認証情報、に基づいて作成される第 2 接続認証情報を、当該接続サーバを特定する情報に関連づけて保持する保持手段と、

前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスを、クライアントアドレスとして取得する手段と、

前記ユーザを特定する情報が、前記第 2 接続認証情報に適合する場合に、当該第 2 接続認証情報に関連づけられた情報により特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出する手段と、

を含み、

前記クライアント装置は、

前記認証用サーバに対し、前記第 2 接続認証情報を、ユーザを特定する情報として、接続要求とともに送信する手段と、

前記認証用サーバから前記接続サーバのアドレスを受信する手段と、

前記受信した接続サーバのアドレスに対し、第 1 接続認証情報を送信する手段と、  
を含み、

前記接続サーバは、

前記認証用サーバから受信したクライアントアドレスからの接続を受け付ける手段と

前記クライアントアドレスから送信される、第 1 接続認証情報を用いて認証処理を行う手段と

を含む、

ことを特徴とするネットワーク接続システム。

**【請求項 2】**

請求項 1 に記載のネットワーク接続システムにおいて、

前記第 2 接続認証情報は、前記第 1 接続認証情報のメッセージダイジェストであることを特徴とするネットワーク接続システム。

**【請求項 3】**

クライアント装置と、接続サーバと、に接続される認証用サーバであって、

前記接続サーバで利用される第 1 接続認証情報、に基づいて作成される第 2 接続認証情報を、当該接続サーバを特定する情報に関連づけて保持する保持手段と、

前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手段と、

前記ユーザを特定する情報が、前記第 2 接続認証情報に適合する場合に、当該第 2 接続認証情報に関連づけられた情報によって特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出する手段と、

を含むことを特徴とする認証用サーバ。

**【請求項 4】**

認証用サーバと、接続サーバと、に接続されるクライアント装置であって、

前記認証用サーバに対して、前記接続サーバで利用される第 1 接続認証情報、に基づいて作成される第 2 接続認証情報とともに接続要求を送信する接続要求手段と、

前記認証用サーバから前記接続サーバのアドレスを受信して、前記受信した接続サーバのアドレスに対し、第 1 接続認証情報を送信する手段と、

を含む

ことを特徴とするクライアント装置。

【請求項 5】

認証用サーバと、クライアント装置と、に接続される接続サーバであって、  
前記認証用サーバから前記クライアント装置のクライアントアドレスを受信して、該クライアントアドレスからの接続を受入可能に制御する手段と、  
当該受入可能となったクライアントアドレスを利用するクライアント装置から認証用情報を受信し、当該認証用情報を用いた認証を行う手段と、  
を含む  
ことを特徴とする接続サーバ。

【請求項 6】

クライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムであって、  
前記認証用サーバは、  
第 1 の暗号化方法で暗号化された第 1 暗号化ユーザ名と第 1 暗号化パスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持する保持手段と、  
前記クライアント装置から接続要求を受信したときに、当該クライアント装置のユーザを特定する情報として、第 1 暗号化ユーザ名及び第 1 暗号化パスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手段と、  
前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、当該接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出する手段と、  
を含み、  
前記クライアント装置は、  
前記認証用サーバに対して、第 1 の暗号化方法で暗号化された第 1 暗号化ユーザ名及び第 1 暗号化パスワードとともに、接続要求を送信する手段と、  
前記認証用サーバから前記接続サーバのネットワークアドレスを受信して、ユーザから入力されたユーザ名と、パスワードとを第 2 の暗号化方法で暗号化して生成した、第 2 暗号化ユーザ名及び第 2 暗号化パスワードを、前記受信したネットワークアドレスに対して送信する手段と、  
を含み、  
前記接続サーバ側で、当該第 2 暗号化ユーザ名及び第 2 暗号化パスワードを用いた認証が行われる  
ことを特徴とするネットワーク接続システム。

【請求項 7】

クライアント装置と、接続サーバと、に接続される認証用サーバであって、  
所定の方法で暗号化されたユーザ名とパスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持する保持手段と、  
前記クライアント装置から接続要求を受信したときに、当該クライアント装置のユーザを特定する情報として、前記暗号化されたユーザ名及びパスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手段と、  
前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、当該接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出する手段と、  
を含むことを特徴とする認証用サーバ。

**【請求項 8】**

認証用サーバと、接続サーバと、に接続されるクライアント装置であって、

前記認証用サーバに対して、第 1 の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信する接続要求手段と、

前記認証用サーバから前記接続サーバのネットワークアドレスを受信して、ユーザから入力されたユーザ名と、パスワードとを第 2 の暗号化方法で暗号化し、当該第 2 の暗号化方法で暗号化したユーザ名及びパスワードを、前記受信したネットワークアドレスに対して送信する手段と、

を含む

ことを特徴とするクライアント装置。

**【請求項 9】**

請求項 8 に記載のクライアント装置であって、

当該クライアント装置に固有の固有情報と、ユーザ名及びパスワードの少なくともいずれか一方とを関連付ける情報として、前記接続サーバから予め提供されているローカル認証用情報を保持する手段と、

ユーザからユーザ名及びパスワードの入力を受け付けると、前記固有情報を生成し、前記ローカル認証用情報を参照して、当該受け付けたユーザ名及びパスワードの少なくともいずれか一方が、前記生成した固有情報に関連付けられているか否かを調べることにより、当該ユーザを認証するローカル認証手段と、

を含み、

前記接続要求手段は、前記ローカル認証手段により、ユーザの認証が行われた場合にのみ、前記認証用サーバに対して、第 1 の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信する

ことを特徴とするクライアント装置。

**【請求項 10】**

クライアント装置と、認証用サーバと、に接続される接続サーバであって、

前記認証用サーバから、接続しようとするクライアント装置のアドレスであるクライアントアドレスの通知を受けて、当該クライアントアドレスからの通信を、予め定められた一定の期間だけ受入可能に設定し、接続待機状態に移行した旨を表す情報を当該認証用サーバに対して送信する

ことを特徴とする接続サーバ。

**【請求項 11】**

クライアント装置と、前記クライアント装置に対して接続先を案内する情報を提供する認証用サーバと、接続サーバとを含むネットワーク接続システムであって、

前記クライアント装置は、当該クライアント装置に固有の第 1 認証情報を演算して、予め前記接続サーバに登録するとともに、前記接続サーバから、当該第 1 認証情報と、所定の第 2 認証情報とを関連付けるローカル認証用情報を取得して保持しており、

ユーザから前記接続サーバに対する接続要求の指示があったときに、前記第 2 認証情報の入力を受けるとともに、クライアント装置に固有の第 1 認証情報を改めて演算し、前記保持しているローカル認証用情報を用いて、入力を受けた第 2 認証情報と、改めて演算した第 1 認証情報との関連づけを調べ、関連付けられていると判断される場合に、前記第 2 認証用情報を第 1 の暗号化方法で暗号化し、前記認証用サーバに対して当該第 1 の暗号化方法で暗号化した第 2 認証用情報を送信し、

前記接続サーバのネットワークアドレスを、接続先を案内する情報として前記認証用サーバから受信して、当該接続サーバのネットワークアドレスに対して、第 2 の暗号化方法で暗号化した第 2 認証用情報を送信して、前記接続サーバとの通信を開始することを特徴とするネットワーク接続システム。

**【請求項 12】**

クライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムを用いた接続方法であって、

前記認証用サーバは、前記接続サーバにおいて利用される第 1 接続認証情報、に基づいて作成される第 2 接続認証情報を、当該接続サーバを特定する情報に関連づけて保持しており、

前記クライアント装置が、前記認証用サーバに対し、前記第 2 接続認証情報を、ユーザを特定する情報として、接続要求とともに送信し、

前記認証用サーバが、前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスを、クライアントアドレスとして取得し、前記ユーザを特定する情報が、前記第 2 接続認証情報に適合する場合に、当該第 2 接続認証情報に関連づけられた情報により特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出し、

前記クライアント装置が、前記認証用サーバから前記接続サーバのアドレスを受信し、当該受信した接続サーバのアドレスに対し、第 1 接続認証情報を送信し、

前記接続サーバが、前記認証用サーバから受信したクライアントアドレスからの接続を受け付けて、当該クライアントアドレスを利用する前記クライアントアドレスから送信される、第 1 接続認証情報を用いて認証処理を行う、

ことを特徴とする接続方法。

#### 【請求項 1 3】

クライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムを用いた接続方法であって、

前記認証サーバは、第 1 の暗号化方法で暗号化されたユーザ名とパスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持しており、

前記クライアント装置が、前記認証用サーバに対して、第 1 の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信し、

前記認証サーバが、当該クライアント装置から接続要求を受信して、当該クライアント装置のユーザを特定する情報として、第 1 の暗号化方法で暗号化されたユーザ名及びパスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得し、前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、

前記接続サーバが、前記認証用サーバから、接続しようとするクライアント装置のアドレスであるクライアントアドレスの通知を受けて、当該クライアントアドレスからの通信を受入可能に設定し、接続待機状態に移行した旨を表す情報を当該認証用サーバに対して送信し、

前記認証用サーバが、前記接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出し、

前記クライアント装置が、前記認証用サーバから受信した、前記接続サーバのネットワークアドレスに対して、ユーザから入力されたユーザ名と、パスワードとを第 2 の暗号化方法で暗号化し、当該第 2 の暗号化方法で暗号化したユーザ名及びパスワードを送信し、

前記接続サーバが、当該クライアント装置から受信した、第 2 の暗号化方法で暗号化されたユーザ名及びパスワードを用いてユーザの認証を行う

ことを特徴とする接続方法。

#### 【請求項 1 4】

クライアント装置と、接続サーバと、に接続される認証用サーバに、

前記接続サーバで利用される第 1 接続認証情報、に基づいて作成される第 2 接続認証情報を、当該接続サーバを特定する情報に関連づけて保持する手順と、

前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワ

ークアドレスをクライアントアドレスとして取得する手順と、

前記ユーザを特定する情報が、前記第2接続認証情報に適合する場合に、当該第2接続認証情報に関連づけられた情報によって特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出する手順と、

を実行させることを特徴とするプログラム。

【請求項15】

認証用サーバと、接続サーバと、に接続されるクライアント装置に、

前記認証用サーバに対して、前記接続サーバで利用される第1接続認証情報、に基づいて作成される第2接続認証情報とともに接続要求を送信する手順と、

前記認証用サーバから前記接続サーバのアドレスを受信して、前記受信した接続サーバのアドレスに対し、第1接続認証情報を送信する手順と、

を実行させることを特徴とするプログラム。

【請求項16】

認証用サーバと、クライアント装置と、に接続される接続サーバに、

前記認証用サーバから前記クライアント装置のクライアントアドレスを受信して、該クライアントアドレスからの接続を受入可能に制御する手順と、

当該受入可能となったクライアントアドレスを利用するクライアント装置から認証用情報を受信し、当該認証用情報を用いた認証を行う手順と、

を実行させることを特徴とするプログラム。

【請求項17】

クライアント装置と、接続サーバと、に接続される認証用サーバに、

所定の方法で暗号化されたユーザ名とパスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持手段に保持する手順と、

前記クライアント装置から接続要求を受信したときに、当該クライアント装置のユーザを特定する情報として、暗号化されたユーザ名及びパスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手順と、

前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、当該接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出する手順と、

を実行させることを特徴とするプログラム。

【請求項18】

認証用サーバと、接続サーバと、に接続されるクライアント装置に、

前記認証用サーバに対して、第1の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信する接続要求手順と、

前記認証用サーバから前記接続サーバのネットワークアドレスを受信して、ユーザから入力されたユーザ名と、パスワードとを第2の暗号化方法で暗号化し、当該第2の暗号化方法で暗号化したユーザ名及びパスワードを、前記受信したネットワークアドレスに対して送信する手順と、

を実行させることを特徴とするクライアント装置用プログラム。

【請求項19】

クライアント装置と、前記クライアント装置との間で暗号化通信を行う認証用サーバとに接続される接続サーバに、

前記認証用サーバから、接続しようとするクライアント装置のアドレスであるクライアントアドレスの通知を受けて、当該クライアントアドレスからの通信を、予め定められた一定の期間だけ受入可能に設定し、接続待機状態に移行した旨を表す情報を当該認証用サーバに対して送信する手順、



を実行させることを特徴とする接続サーバ用プログラム。

**【書類名】明細書****【発明の名称】** ネットワーク接続システム**【技術分野】****【0001】**

本発明は、ローカルネットワーク等にリモートからの接続を可能とするネットワーク接続システムに関する。

**【背景技術】****【0002】**

近年では、インターネット接続環境の普及と相俟って、個々人のワーキングスタイルが多様化しつつある。例えば、企業に属しながら自宅で仕事を行う、いわゆる在宅型のワーキングスタイルも受け入れられ易くなってきている。これは、企業内のローカルネットワークに対してインターネットや公衆電話回線網等、異なるユーザが共用するネットワークを経由して、自宅等、遠隔地からアクセスする、いわゆるリモートアクセスサービス（RAS）技術の開発が進展してきたからである。

**【0003】**

こうしたリモートアクセスサービスでは、企業内で利用される情報が、外部から自由に参照されることを防止するため、予めローカルネットワークに登録されたユーザ名と、パスワードとによってローカルネットワーク側で認証を行うとともに、遠隔地とアクセス先であるローカルネットワークとの間のネットワーク（途中のネットワーク）上での認証後のトラフィックを暗号化しているのが普通である。

**【0004】**

なお、複数のサーバのユーザ認証情報を保持していない端末からも、それらをアクセスでき、各サーバの課金をまとめて管理するシステムを提供する目的で、中間サーバから各端末が、接続先となるサーバへの接続に必要な情報を取得する技術が特許文献1に開示されている。

**【特許文献1】** 特開平08-235114号公報

**【発明の開示】****【発明が解決しようとする課題】****【0005】**

しかしながら、上記従来のリモートアクセスサービスでは、認証後のトラフィックは暗号化されるものの、ユーザ名等の認証用の情報はそのまま流通する。従って、ユーザ名が途中のネットワークで不正に取得された場合、ローカルネットワーク側に対して、当該不正に取得したユーザ名を送出し、パスワードとしてランダムにアタックをしかけるタイプの不正アクセスが可能になる。

**【0006】**

本発明は上記実情に鑑みて為されたもので、リモートアクセスにおけるセキュリティを向上できるネットワーク接続システムを提供することを、その目的の一つとする。

**【課題を解決するための手段】****【0007】**

上記従来例の問題点を解決するための本発明は、クライアント装置と、認証用サーバと、接続サーバを含むネットワーク接続システムであって、前記認証用サーバは、前記接続サーバにおいて利用される第1接続認証情報、に基づいて作成される第2接続認証情報を、当該接続サーバを特定する情報に関連づけて保持する保持手段と、前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスを、クライアントアドレスとして取得する手段と、前記ユーザを特定する情報が、前記第2接続認証情報に適合する場合に、当該第2接続認証情報に関連づけられた情報により特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出する手段と、を含み、前記クライアント装置は、前記認証用サーバに対し、前記第2接続認

証情報を、ユーザを特定する情報として、接続要求とともに送信する手段と、前記認証用サーバから前記接続サーバのアドレスを受信する手段と、前記受信した接続サーバのアドレスに対し、第1接続認証情報を送信する手段と、を含み、前記接続サーバは、前記認証用サーバから受信したクライアントアドレスからの接続を受け付ける手段と前記クライアントアドレスから送信される、第1接続認証情報を用いて認証処理を行う手段とを含む、ことを特徴としている。

【0008】

またここで、前記第2接続認証情報は、前記第1接続認証情報のメッセージダイジェストであることとしてもよい。

【0009】

また上記従来例の問題点を解決するための本発明は、クライアント装置と、接続サーバと、に接続される認証用サーバであって、前記接続サーバで利用される第1接続認証情報、に基づいて作成される第2接続認証情報を、当該接続サーバを特定する情報に関連づけて保持する保持手段と、前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手段と、前記ユーザを特定する情報が、前記第2接続認証情報に適合する場合に、当該第2接続認証情報に関連づけられた情報によって特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出する手段と、を含むことを特徴としている。

【0010】

また、上記従来例の問題点を解決するための本発明は、認証用サーバと、接続サーバと、に接続されるクライアント装置であって、前記認証用サーバに対して、前記接続サーバで利用される第1接続認証情報、に基づいて作成される第2接続認証情報とともに接続要求を送信する接続要求手段と、前記認証用サーバから前記接続サーバのアドレスを受信して、第1接続認証情報を、前記受信した接続サーバのアドレスに対して送信する手段と、を含むことを特徴としている。

【0011】

また、上記従来例の問題点を解決するための本発明は、認証用サーバと、クライアント装置と、に接続される接続サーバであって、前記認証用サーバから前記クライアント装置のクライアントアドレスを受信して、該クライアントアドレスからの接続を受入可能に制御する手段と、当該受入可能となったクライアントアドレスを利用するクライアント装置から認証用情報を受信し、当該認証用情報を用いた認証を行う手段と、を含むことを特徴としている。

【0012】

また、本発明のある態様に係るクライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムでは、前記認証用サーバは、第1の暗号化方法で暗号化された第1暗号化ユーザ名と第1暗号化パスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持する保持手段と、前記クライアント装置から接続要求を受信したときに、当該クライアント装置のユーザを特定する情報として、第1暗号化ユーザ名及び第1暗号化パスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手段と、前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連づけられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、当該接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出する手段と、を含み、前記クライアント装置は、前記認証用サーバに対して、第1の暗号化方法で暗号化された第1暗号化ユーザ名及び第1暗号化パスワードとともに、接続要求を送信する手段と、前記認証用サーバから前記接続サーバのネットワークアドレスを受信して、ユーザから入力されたユーザ名と、パスワードとを第2の暗号化方法で暗号化し

て生成した、第2暗号化ユーザ名及び第2暗号化パスワードを、前記受信したネットワークアドレスに対して送信する手段と、を含み、前記接続サーバ側で、当該第2暗号化ユーザ名及び第2暗号化パスワードを用いた認証が行われることを特徴としている。

#### 【0013】

このようにしたので、クライアント装置のユーザは、認証用サーバにおいて認証を受けるまでは、接続サーバのネットワークアドレスを知ることができない。さらに、認証サーバ及び接続サーバに対して送出されるユーザ名等は、それぞれ第1、第2の暗号化方法、例えばハッシュ関数によって暗号化されたり、所与のランダム情報をユーザ名等をキーとして暗号化するといった方法で暗号化されているため、ユーザ名等が漏えいすることが防止され、セキュリティを向上させることができる。なお、第1、第2の暗号化方法は互いに異なる方法であってもよいし、同じ方法であってもよい。

#### 【0014】

上記従来例の問題点を解決するための本発明は、クライアント装置と、接続サーバと、に接続される認証用サーバであって、所定の方法で暗号化されたユーザ名とパスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持する保持手段と、前記クライアント装置から接続要求を受信したときに、当該クライアント装置のユーザを特定する情報として、前記暗号化されたユーザ名及びパスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手段と、前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、当該接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出する手段と、を含むことを特徴としている。

#### 【0015】

また上記従来例の問題点を解決するための本発明は、認証用サーバと、接続サーバと、に接続されるクライアント装置であって、前記認証用サーバに対して、第1の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信する接続要求手段と、前記認証用サーバから前記接続サーバのネットワークアドレスを受信して、ユーザから入力されたユーザ名と、パスワードとを第2の暗号化方法で暗号化し、当該第2の暗号化方法で暗号化したユーザ名及びパスワードを、前記受信したネットワークアドレスに対して送信する手段と、を含むことを特徴としている。

#### 【0016】

ここで、このクライアント装置は、クライアント装置に固有の固有情報と、ユーザ名及びパスワードの少なくともいずれか一方とを関連付ける情報として、前記接続サーバから予め提供されているローカル認証用情報を保持する手段と、ユーザからユーザ名及びパスワードの入力を受け付けると、前記固有情報を生成し、前記ローカル認証用情報を参照して、当該受け付けたユーザ名及びパスワードの少なくともいずれか一方が、前記生成した固有情報に関連付けられているか否かを調べることにより、当該ユーザを認証するローカル認証手段と、を含み、前記接続要求手段は、前記ローカル認証手段により、ユーザの認証が行われた場合にのみ、前記認証用サーバに対して、第1の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信することとしてもよい。

#### 【0017】

また、上記従来例の問題点を解決するための本発明は、クライアント装置と、認証用サーバと、に接続される接続サーバであって、前記認証用サーバから、接続しようとするクライアント装置のアドレスであるクライアントアドレスの通知を受けて、当該クライアントアドレスからの通信を、予め定められた一定の期間だけ受入可能に設定し、接続待機状態に移行した旨を表す情報を当該認証用サーバに対して送信することを特徴としている。

#### 【0018】

さらに、上記従来例の問題点を解決するための本発明は、クライアント装置と、前記クライアント装置に対して接続先を案内する情報を提供する認証用サーバと、接続サーバと

を含むネットワーク接続システムであって、前記クライアント装置は、当該クライアント装置に固有の第1認証情報を演算して、予め前記接続サーバに登録するとともに、前記接続サーバから、当該第1認証情報と、所定の第2認証情報とを関連付けるローカル認証用情報を取得して保持しており、ユーザから前記接続サーバに対する接続要求の指示があったときに、前記第2認証情報の入力を受けるとともに、クライアント装置に固有の第1認証情報を改めて演算し、前記保持しているローカル認証用情報を用いて、入力を受けた第2認証用情報と、改めて演算した第1認証用情報との関連づけを調べ、関連付けられていると判断される場合に、前記第2認証用情報を第1の暗号化方法で暗号化し、前記認証用サーバに対して当該第1の暗号化方法で暗号化した第2認証用情報を送信し、前記接続サーバのネットワークアドレスを、接続先を案内する情報として前記認証用サーバから受信して、当該接続サーバのネットワークアドレスに対して、第2の暗号化方法で暗号化した第2認証用情報を送信して、前記接続サーバとの通信を開始することとしている。

#### 【0019】

また、本発明の一態様に係る、クライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムを用いた接続方法は、前記認証用サーバが、前記接続サーバにおいて利用される第1接続認証情報、に基づいて作成される第2接続認証情報を、当該接続サーバを特定する情報に関連づけて保持しており、前記クライアント装置が、前記認証用サーバに対し、前記第2接続認証情報を、ユーザを特定する情報として、接続要求とともに送信し、前記認証用サーバが、前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスを、クライアントアドレスとして取得し、前記ユーザを特定する情報が、前記第2接続認証情報に適合する場合に、当該第2接続認証情報に関連づけられた情報により特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出し、前記クライアント装置が、前記認証用サーバから前記接続サーバのアドレスを受信し、当該受信した接続サーバのアドレスに対し、第1接続認証情報を送信し、前記接続サーバが、前記認証用サーバから受信したクライアントアドレスからの接続を受け付けて、当該クライアントアドレスを利用する前記クライアントアドレスから送信される、第1接続認証情報を用いて認証処理を行うものである。

#### 【0020】

さらに、本発明の一態様に係る、ネットワークへの接続方法は、クライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムを用いた接続方法であって、前記認証サーバは、第1の暗号化方法で暗号化されたユーザ名とパスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持しており、前記クライアント装置が、前記認証用サーバに対して、第1の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信し、前記認証サーバが、当該クライアント装置から接続要求を受信して、当該クライアント装置のユーザを特定する情報として、第1の暗号化方法で暗号化されたユーザ名及びパスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得し、前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、前記接続サーバが、前記認証用サーバから、接続しようとするクライアント装置のアドレスであるクライアントアドレスの通知を受けて、当該クライアントアドレスからの通信を受入可能に設定し、接続待機状態に移行した旨を表す情報を当該認証用サーバに対して送信し、前記認証用サーバが、前記接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出し、前記クライアント装置が、前記認証用サーバから受信した、前記接続サーバのネットワークアドレスに対して、ユーザから入力されたユーザ名と、パスワードとを第2の暗号化方法で暗号化し、当該第2の暗号化方法で暗号化

したユーザ名及びパスワードを送信し、前記接続サーバが、当該クライアント装置から受信した、第2の暗号化方法で暗号化されたユーザ名及びパスワードを用いてユーザの認証を行うことを特徴としている。

#### 【0021】

また、上記従来例の問題点を解決するための本発明は、クライアント装置と、接続サーバと、に接続される認証用サーバにより実行されるプログラムであって、前記接続サーバで利用される第1接続認証情報、に基づいて作成される第2接続認証情報を、当該接続サーバを特定する情報に関連づけて保持する手順と、前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手順と、前記ユーザを特定する情報が、前記第2接続認証情報に適合する場合に、当該第2接続認証情報に関連づけられた情報によって特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出する手順と、を前記認証用サーバに実行させることを特徴としている。

#### 【0022】

また、上記従来例の問題点を解決するための本発明は、認証用サーバと、接続サーバと、に接続されるクライアント装置により実行されるプログラムであって、前記認証用サーバに対して、前記接続サーバで利用される第1接続認証情報、に基づいて作成される第2接続認証情報とともに接続要求を送信する手順と、前記認証用サーバから前記接続サーバのアドレスを受信して、前記受信した接続サーバのアドレスに対し、第1接続認証情報を送信する手順と、を前記クライアント装置に実行させることを特徴としている。

#### 【0023】

さらに、上記従来例の問題点を解決するための本発明は、認証用サーバと、クライアント装置と、に接続される接続サーバによって実行されるプログラムであって、前記認証用サーバから前記クライアント装置のクライアントアドレスを受信して、該クライアントアドレスからの接続を受入可能に制御する手順と、当該受入可能となったクライアントアドレスを利用するクライアント装置から認証用情報を受信し、当該認証用情報を用いた認証を行う手順と、を前記接続サーバに実行させることを特徴としている。

#### 【0024】

また、上記従来例の問題点を解決するための本発明は、クライアント装置と、接続サーバと、に接続される認証用サーバに、所定の方法で暗号化されたユーザ名とパスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持手段に保持する手順と、前記クライアント装置から接続要求を受信したときに、当該クライアント装置のユーザを特定する情報として、暗号化されたユーザ名及びパスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手順と、前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、当該接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出する手順と、を実行させることを特徴としている。

#### 【0025】

さらに、上記従来例の問題点を解決するための本発明は、認証用サーバと、接続サーバと、に接続されるクライアント装置に、前記認証用サーバに対して、第1の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信する接続要求手順と、前記認証用サーバから前記接続サーバのネットワークアドレスを受信して、ユーザから入力されたユーザ名と、パスワードとを第2の暗号化方法で暗号化し、当該第2の暗号化方法で暗号化したユーザ名及びパスワードを、前記受信したネットワークアドレスに対して送信する手順と、を実行させることを特徴としている。

#### 【0026】

さらに上記従来例の問題点を解決するための本発明は、クライアント装置と、前記クライアント装置との間で暗号化通信を行う認証用サーバとに接続される接続サーバに、前記認証用サーバから、接続しようとするクライアント装置のアドレスであるクライアントアドレスの通知を受けて、当該クライアントアドレスからの通信を、予め定められた一定の期間だけ受入可能に設定し、接続待機状態に移行した旨を表す情報を当該認証用サーバに対して送信する手順、を実行させることを特徴としている。

【発明を実施するための最良の形態】

#### 【0027】

本発明の実施の形態について図面を参照しながら説明する。本発明の実施の形態に係るネットワーク接続システムは、図1に示すように、ローカルネットワーク1と、公衆ネットワーク2と、この公衆ネットワーク2に接続されたクライアント装置3と、認証サーバ4とを含んで構成されている。ローカルネットワーク1は、接続サーバ11を介して公衆ネットワーク2に接続されている。公衆ネットワーク2は、インターネットや公衆電話回線網などからなるネットワークシステムである。なお図1では認証サーバ4は一つしか図示していないが、認証サーバ4は複数あっても構わない。

#### 【0028】

クライアント装置3は、一般的なパーソナルコンピュータであり、図1に示したように制御部31と、記憶部32と、通信制御部33と、表示部34と、操作部35とを含む。制御部31は、記憶部32に格納されているプログラム（クライアント装置用プログラム）に従って動作している。この制御部31は、ローカルネットワーク1へのRAS接続処理を実行する。このRAS接続処理の具体的内容については後に詳しく述べる。記憶部32は、プログラムなどを格納する、コンピュータ読み取り可能な記憶媒体である。この記憶部32は、また、制御部31のワークメモリとしても動作する。

#### 【0029】

通信制御部33は、制御部31から入力される指示に従って、当該指示に含まれるネットワークアドレスで特定される宛先に対して情報を送信する。また、この通信制御部33は、ネットワークを介して到来する情報を受信して制御部31に出力する。表示部34は、制御部31から入力される指示に従って情報を表示するディスプレイ装置などである。操作部35は、キーボードやマウスなどであり、ユーザの指示操作の内容を制御部31に対して出力する。

#### 【0030】

認証サーバ4は、一般的なサーバコンピュータであり、制御部41と、記憶部42と、通信制御部43とを含んで構成される。制御部41は、記憶部42に格納されているプログラム（認証サーバ用プログラム）に従って動作し、認証処理を行う。この認証処理の具体的内容については後に詳しく述べる。

#### 【0031】

記憶部42は、プログラムなどを格納する、コンピュータ読み取り可能な記憶媒体である。この記憶部42はまた、制御部41のワークメモリとしても動作する。通信制御部43は、制御部41から入力される指示に従って、当該指示に含まれるネットワークアドレスで特定される宛先に対して情報を送信する。また、この通信制御部43は、ネットワークを介して到来する情報を受信して制御部41に出力する。

#### 【0032】

また、ローカルネットワーク1の接続サーバ11もまた、一般的なサーバコンピュータであってよく、制御部15と、記憶部16と、第1通信制御部17と、第2通信制御部18とを含んで構成される。制御部15は、記憶部16に格納されているプログラム（接続サーバ用プログラム）に従って動作し、認証処理と接続処理等を行う。これらの認証処理や接続処理の具体的内容については後に詳しく述べる。

#### 【0033】

記憶部16は、プログラムなどを格納する、コンピュータ読み取り可能な記憶媒体である。この記憶部16はまた、制御部15のワークメモリとしても動作する。第1通信制御

部 17 は、制御部 15 から入力される指示に従って、当該指示に含まれるネットワークアドレスで特定される宛先に対し、公衆ネットワーク 2 を介して情報を送信する。また、この第 1 通信制御部 17 は、公衆ネットワーク 2 を介して到来する情報を受信して制御部 15 に出力する。第 2 通信制御部 18 は、制御部 15 から入力される指示に従って、当該指示に含まれるネットワークアドレスで特定される宛先に対し、ローカルネットワーク 1 を介して情報を送信する。また、この第 2 通信制御部 18 は、ローカルネットワーク 1 を介して到来する情報を受信して制御部 15 に出力する。

#### 【0034】

この接続サーバ 11 の制御部 15 は、後に説明する方法で認証したクライアント装置 3 から、第 1 通信制御部 17 を介して受信する、データの要求などを第 2 通信制御部 18 を介してローカルネットワーク 1 側に伝達する。また、ローカルネットワーク 1 側からクライアント装置 3 へ送信すべきデータ等を第 2 通信制御部 18 を介して受け入れ、第 1 通信制御部 17 を介して送信する。

#### 【0035】

##### [セットアップ]

ここで、クライアント装置 3 と、認証サーバ 4 と、接続サーバ 11 との間で行われる認証処理について説明する。まず、クライアント装置 3 が、接続サーバ 11 を介して RAS 接続可能となるまでのセットアップの手順を述べる。なお、以下の説明において、クライアント装置 3 と認証サーバ 4 との間の通信は、広く知られた SSL (Secure Socket Layer) などの方法で暗号化されていることとしてもよい。

#### 【0036】

本実施の形態において特徴的なことの一つは、クライアント装置 3 に対して RAS 接続のための専用のアプリケーションソフトウェアがインストールされることである。この専用アプリケーションソフトウェアは、暗号化された認証サーバ 4 のネットワークアドレスを保持しており、また、当該暗号化された認証サーバ 4 のネットワークアドレスを復号する手順をクライアント装置 3 に実行させ、クライアント装置 3 は、この専用アプリケーションソフトウェアによらなければ、認証サーバ 4 に対するアクセスが事実上できないようになっている。

#### 【0037】

次に、この専用アプリケーションソフトウェアのセットアップ手順を説明する。クライアント装置 3 に、この専用アプリケーションソフトウェアがインストールされると、クライアント装置 3 は、当該クライアント装置に固有の第 1 認証情報として、クライアント装置 3 を構成するハードディスクのシリアル番号など、ハードウェア関係情報や、オペレーティングシステムのバージョンなどソフトウェア環境に関する情報といったクライアント装置 3 ごとに一般に異なる情報に基づいて、クライアント装置 3 の固有情報を演算する。

#### 【0038】

ユーザは、この固有情報と、ユーザ名、パスワードといった情報を接続サーバ 11 の管理者に伝達する。この伝達方法は、例えば暗号化した電子メールであってもよいし、磁気ディスク等を利用した伝達手段によってもよい。接続サーバ 11 の管理者は、これら固有情報、ユーザ名、パスワードを接続サーバ 11 に登録する。接続サーバ 11 は、この登録を受けて、当該ユーザを認証する認証サーバ 4 を選定し、当該選定した認証サーバ 4 のネットワークアドレスを暗号化して暗号化アドレスを生成し、また、所定の情報（任意の文字列でもよいし、RAS 接続の有効期限などといった意味ある情報でもよい）を、固有情報をキーとして暗号化した第 1 情報と、当該所定の情報を、ユーザ名をキーとして暗号化した第 2 情報とを生成する。そして接続サーバ 11 は、これら暗号化アドレスと、第 1 情報と、第 2 情報とを含む情報を、定義情報として出力する。これら第 1 情報と第 2 情報とが、第 1 認証情報と第 2 認証情報とを関連付けるローカル認証用情報に相当する。またこの定義情報には、パスワードを、後に説明する第 1 の暗号化方法で暗号化した、暗号化パスワードの少なくとも一部を含んでもよい。



## 【0039】

この定義情報は、クライアント装置3のユーザへの電子メール等、任意の方法でクライアント装置3側に提供され、クライアント装置3の記憶部32に格納される。クライアント装置3は、専用アプリケーションソフトウェアに従って、この定義情報を利用して固有情報が誤りなく登録されたか否かを調べる。具体的には、固有情報を演算して生成するとともにユーザに対してユーザ名を入力させ、第1情報を生成した固有情報で復号し、第2情報を当該入力されたユーザ名で復号する。そしてこれらの復号結果（正しく復号されればいずれも上記所定の情報となる）が互いに一致するか否かを調べ、一致する場合に、固有情報が誤りなく登録されたと判断する。

## 【0040】

一方、接続サーバ11は、第1通信制御部17側に割り当てられているネットワークアドレス（公衆ネットワーク側のアドレス）と、クライアント装置3のユーザ名及びパスワードを第1の暗号化方法で暗号化したものとを認証サーバ4に対して送信する。ここでのユーザ名及びパスワードの暗号化方法（第1の暗号化方法）は、復号可能なものでなくてもよく、ユーザ名及びパスワードのそれぞれについてのMD5等のハッシュ値を用いるなど、メッセージダイジェストを利用してもよい。認証サーバ4は、図2に示すように、当該接続サーバ11から受信したネットワークアドレスと、第1の暗号化方法で暗号化されたユーザ名及びパスワードを関連付けて、保持手段としての記憶部42に格納する。こうして一連のセットアップが完了する。

## 【0041】

## [認証処理]

次に、実際に接続要求が為された場合の認証処理について図3及び図4を参照しながら説明する。ユーザはローカルネットワーク1側にRAS接続しようとするときに、クライアント装置3にインストールされている専用アプリケーションソフトウェアを起動する。まず、図3に示すようにクライアント装置3の制御部31は、専用アプリケーションソフトウェアに従って、ユーザに対してユーザ名とパスワードとを入力するよう表示部34に表示する（S1）。ユーザが操作部35を操作して、第2認証情報（本発明の第1接続認証情報にも対応する）としてのユーザ名とパスワードとを入力すると（S2）、第1認証情報としての固有情報を演算して生成し（S3）、第1情報を生成した固有情報で復号し、第2情報を当該入力されたユーザ名で復号する。そしてこれらの復号結果が互いに一致するか否かを調べ（S4）、一致したときに、処理S2で入力されたユーザ名及びパスワードを第1の暗号化方法で暗号化する（S5）。この第1の暗号化方法で暗号化されたユーザ名及びパスワードが本発明の第2接続認証情報に対応する。またこのとき、定義情報に、暗号化パスワードの少なくとも一部が含まれる場合は、処理S5で暗号化したパスワードのうち対応する少なくとも一部と、定義情報に含まれている上記暗号化パスワードの少なくとも一部とが一致するか否かを比較し、一致しない場合は処理を中断してもよい。なお、暗号化したパスワードの全体で比較しないことにより、セキュリティがさらに向上する。

## 【0042】

また制御部31は、認証サーバ4のネットワークアドレスを復号し（S6）、復号して得たネットワークアドレスに対して、処理S5にて第1の暗号化方法で暗号化した第1暗号化ユーザ名及び第1暗号化パスワードとともに、接続要求を送信する（S7）。なお、処理S4において一致しなかった場合は、その時点で認証処理を中断する。

## 【0043】

本実施の形態において特徴的なことの一つは、専用アプリケーションソフトウェアの処理として、処理S3に示すように、RAS接続をしようとするごとに毎回、第1認証情報としての固有情報の演算を改めて行うことである。これにより他の認証情報が漏洩したとしても、一般に異なるコンピュータを用いた場合は異なる第1認証情報が演算される結果となるため、RAS接続の処理が中断される。

## 【0044】

認証サーバ4は、クライアント装置3から接続要求とともに受信した、暗号化されたユーザ名及びパスワードを受信し、記憶部42を参照して、当該暗号化されたユーザ名及びパスワードを検索する(S11)。ここで、当該暗号化されたユーザ名及びパスワードが記憶部42に格納されていた場合は、当該暗号化されたユーザ名及びパスワードに関連付けられている、接続サーバ11のネットワークアドレスを取得する(S12)。なお、処理S11にて当該暗号化されたユーザ名及びパスワードが記憶部42に格納されていなかった場合(これらによる認証に失敗した場合)は、認証サーバ4は処理S12以降の処理を行うことなく、処理を終了する。

#### 【0045】

また、認証サーバ4は、接続要求元のクライアント装置3のネットワークアドレス(クライアントアドレス)を取得する(S13)。認証サーバ4は、処理S12で取得した接続サーバ11のネットワークアドレスに対して、処理S13で取得したクライアントアドレスを送信して(S14)、接続サーバ11から接続待機状態に移行した旨を表す情報を受信するまで待機する(S15)。このフローの続きは、図示の都合上、図4に示されている。

#### 【0046】

図4に上記フローの続きを示すように、接続サーバ11は、認証サーバ4からクライアントアドレスを受信すると、当該ネットワークアドレスからのアクセスを、予め定められた一定の期間だけ受入可能に設定する(S21)。この認証サーバ4と接続サーバ11との間の通信は、専用回線や暗号化通信回線など、セキュアな回線を用いて行われることとしてもよい。具体的にクライアント装置3とのRAS接続を、pptp(Point-to-Point Tunneling Protocol)を用いて行う場合、接続サーバ11にファイアウォールを設定しておき、認証サーバ4からクライアント装置3のネットワークアドレスを受信したときに、pptpのポート(TCPのポート)を一定の期間(例えば60秒)だけオープンする。そして、接続サーバ11は、接続待機状態に移行した旨を認証サーバ4に対して送信する(S22)。

#### 【0047】

認証サーバ4は、接続サーバ11から接続待機状態に移行した旨を表す情報を受信すると、クライアント装置3に対して接続の指示を送信する(S31)。クライアント装置3は接続の指示を受信すると、第2認証情報としてのユーザ名とパスワードとを第2の暗号化方法で暗号化して(S41)、この第2の暗号化方法で暗号化した第2暗号化ユーザ名と第2暗号化パスワードとをpptpにおけるユーザ名及びパスワードとして接続サーバ11に送信する(S42)。

#### 【0048】

ここで、処理S31の接続の指示には、接続サーバ11のネットワークアドレスを含めてもよい。この場合、接続サーバ11のネットワークアドレスを、クライアント装置3に事前に設定しておく必要がない。また、この場合クライアント装置3は、処理S42において、受信した接続の指示に含まれるネットワークアドレスで特定される接続サーバ11に、第2の暗号化方法で暗号化した第2暗号化ユーザ名と第2暗号化パスワードとを送信することになる。これにより、クライアント装置のユーザは、認証用サーバにおいて認証を受けるまでは、接続サーバのネットワークアドレスを知ることもできないこととなり、セキュリティを向上できる。

#### 【0049】

なお、ここでは接続サーバ11が接続待機状態に移行した旨を認証サーバ4に対して送信することとしているが、この送信は必ずしも必要ではない。この送信が行われない場合は、認証サーバ4は接続サーバ11に対してクライアントアドレスを送信し、クライアント装置3に対して接続の指示を送信する処理(処理S31)を行う。

#### 【0050】

接続サーバ11は、この暗号化されたユーザ名とパスワードとが、登録されているユーザ名とパスワードに一致しているか否かを調べ(S51)、一致している場合は、ppt

pによる通信を開始する(S52)。また、処理S51において一致していない場合は、認証処理を中断する。ここでの第2の暗号化方法による暗号化も、必ずしも復号可能である必要はなく、例えばユーザ名のハッシュ値とパスワードのハッシュ値としてもよい(すなわち第1の暗号化方法と同じ方法であってもよい)し、所定の情報(例えば固有情報など、接続要求のたびに生成される情報や、接続サーバ11側から取得されるチャレンジ情報(接続要求のたびに生成されるランダム値を含む情報))をユーザ名やパスワードをキーとしてそれぞれ暗号化したものであってもよい。

#### 【0051】

接続サーバ11側では、ユーザ名等がMD5などのハッシュ値として暗号化される場合は、登録されたユーザ名等のハッシュ値と比較することにより、一致するか否かを調べてユーザ名等の認証を行う。また、ユーザ名等をキーとして固有情報が暗号化されている場合は、登録されているユーザ名等と固有情報とを用いて同じように暗号化を行い、第2暗号化ユーザ名等を生成して、当該生成したものが受信したものと一致するか否かを調べてユーザ名等の認証を行う。

#### 【0052】

さらに、チャレンジ情報を用いる場合は、ランダム情報を含むチャレンジ情報を発行し、クライアント装置3側に当該発行したチャレンジ情報を提供し、ユーザ名等をキーとして暗号化されたチャレンジ情報を受信し、登録されているユーザ名等と発行したチャレンジ情報とを用いて同じように暗号化を行い、第2暗号化ユーザ名等を生成して、当該生成したものが受信したものと一致するか否かを調べてユーザ名等の認証を行う。

#### 【0053】

##### [接続処理]

このようにして認証が行われるため、たとえ途中で暗号化されたユーザ名やパスワードが漏洩したとしても、元のユーザ名を知ることは困難であるので、専用アプリケーションソフトウェアを操作することができない。また接続サーバ11のポートをオープンさせるためには、認証サーバ4に対する攻撃が不可欠であり、接続サーバ11に対する攻撃の頻度を低下させるうえ、基本的な認証が認証サーバ4にてまず行われることで、接続サーバ11の処理負荷の軽減にも資している。さらに、仮にポートをオープンさせ、パスワード等の大量送信によるハッキングが可能となったとしても、ポートがオープンしている60秒以内に、ユーザ名とパスワードとを調べあげる必要があるなど、事実上不正アクセスはできない。さらに、接続処理が完了したときには、当該接続に用いられたポートを閉じるようにしてもよい。また、接続サーバ11のポートがオープンしている状態で、パスワードなどによる認証にあらかじめ定めた回数(例えば1回としてもよい)だけ失敗するとポートを閉じるようにしてもよい。

#### 【0054】

本実施の形態において、さらに特徴的なことの一つは、接続要求のたびに生成される情報を利用して、ユーザ名やパスワードの暗号化が行われるにもかかわらず、当該暗号化されたユーザ名によってユーザを特定できることである。従ってローカルネットワーク側では、ユーザごとにアクセス権を設定するなど、ユーザごとに対応した処理が可能となる。

#### 【0055】

また、接続サーバ11は、ユーザごとに最終アクセス日時などのアクセス記録を生成し、記憶部16に格納しておいてもよい。この場合、ユーザからアクセスが行われるごとに、当該ユーザに対して、当該ユーザが前回アクセスした日時の情報を記憶部16から検索して提供する。これにより各利用者は、万が一、不正アクセスがあった場合でも、その事実を認識でき、セキュリティがより向上する。

#### 【0056】

またこのように、ユーザを特定できるので、ユーザごとに期限を設定することとしても好ましい。具体的には、接続サーバ11はユーザごとに期限の情報を関連付けて保持しており、p p t pによる通信を開始する前に、処理S51にて認証したユーザの期限の情報と、図示しないカレンダーの情報とを参照し、期限が到来しているか否かを調べ、到来して

いれば認証処理を中断して、接続を拒否し、到来していない場合は処理 S 5 2 に移行して p p t p による通信を開始する。この期限の情報は、接続サーバ 1 1 の管理者が更新して登録できるようにしておいてもよい。

#### 【0057】

なお、ここまでの説明では、クライアント装置 3 は、処理 S 5 から S 7 により、第 1 暗号化ユーザ名及び第 1 暗号化パスワードとともに、接続要求を送信するようにしているが、まず第 1 暗号化ユーザ名とともに接続要求を送信し、認証サーバ 4 がこの接続要求を受けて発行したチャレンジ情報（ランダム情報を含む）を受信して、当該チャレンジ情報を第 1 暗号化パスワードをキーとして暗号化して送信するなど、パスワードについては、いわゆるチャレンジレスポンスを利用した認証を行ってもよい。

#### 【0058】

このことは、接続サーバ 1 1 との間でも同様であり、ここまでの説明では第 2 の暗号化方法で暗号化した第 2 暗号化ユーザ名と、第 2 暗号化パスワードとを生成して接続サーバ 1 1 に対して送信していたが、パスワードについては、第 2 の暗号化方法による暗号化をすることなく、一部の p p t p において実装されている、チャレンジレスポンスを利用した認証を行うようにしてもよい。

#### 【0059】

また、接続サーバ 1 1 の第 1 通信制御部 1 7 のネットワークアドレスは、固定的に設定されていても、時間とともに変化してもよい。すなわち、ここでいうネットワークアドレスが I P アドレスである場合、スタティックであっても、ダイナミックであっても構わない。接続サーバ 1 1 は、自己の第 1 通信制御部 1 7 に割り当てられるネットワークアドレスが変更されたときには、変更後のネットワークアドレスを認証サーバ 4 に対して送信してその登録を更新させる。

#### 【0060】

さらに、ここでは、クライアント装置 3 との R A S 接続の通信プロトコルとして p p t p を用いる例について述べたが、これに限らず、I P S E C や V P N - H T T P S 等、他のセキュアな通信プロトコルを用いても構わない。

#### 【図面の簡単な説明】

#### 【0061】

【図 1】本発明の実施の形態に係るネットワーク接続システムの例を表す構成ブロック図である。

【図 2】認証サーバ内に格納されているデータの一例を表す説明図である。

【図 3】本発明の実施の形態に係るネットワーク接続の前半部分の流れの例を表すフロー図である。

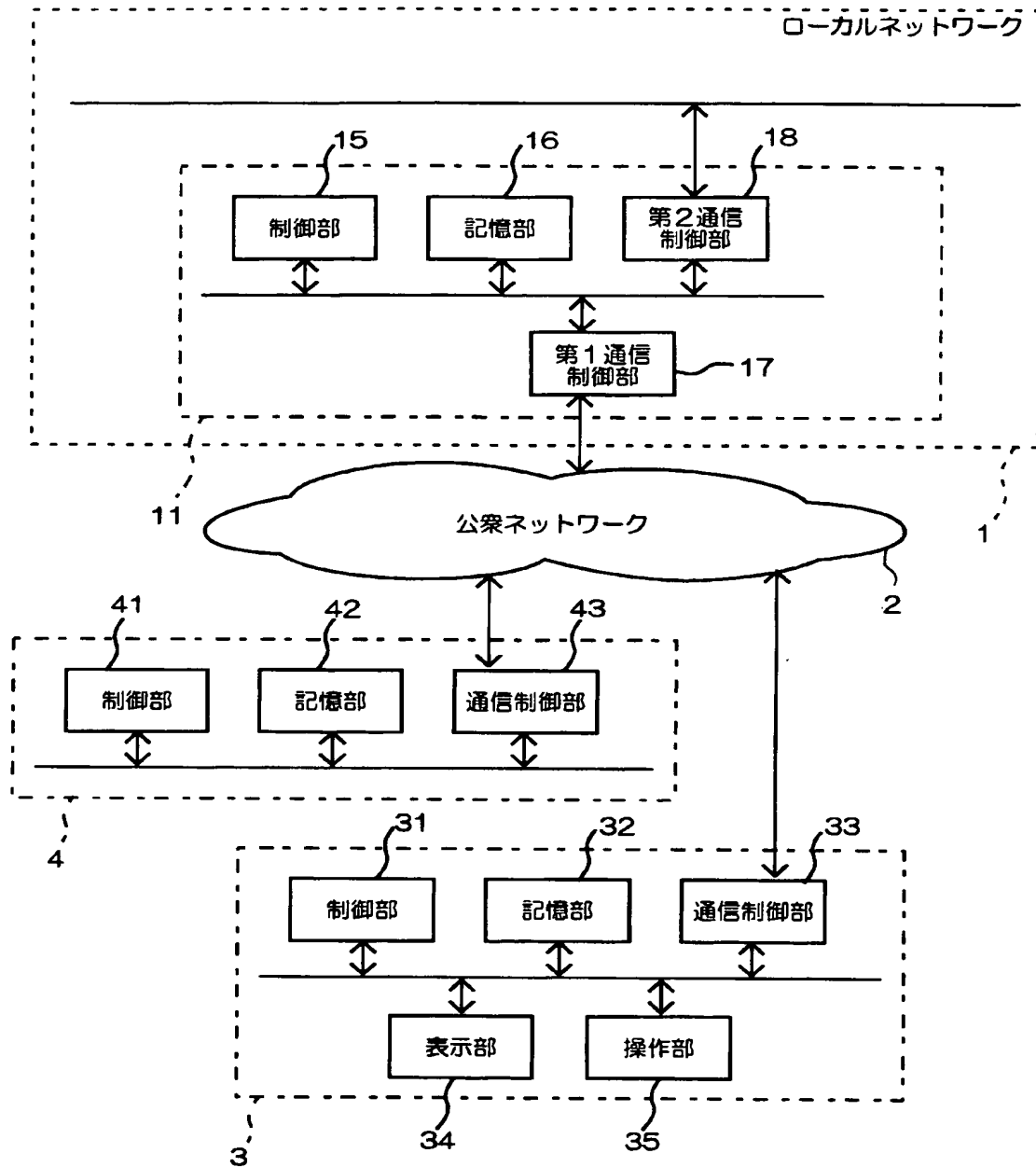
【図 4】本発明の実施の形態に係るネットワーク接続の後半部分の流れの例を表すフロー図である。

#### 【符号の説明】

#### 【0062】

1 ローカルネットワーク、2 公衆ネットワーク、3 クライアント装置、4 認証サーバ、1 1 接続サーバ、1 5, 3 1, 4 1 制御部、1 6, 3 2, 4 2 記憶部、1 7 第 1 通信制御部、1 8 第 2 通信制御部、3 3, 4 3 通信制御部、3 4 表示部、3 5 操作部。

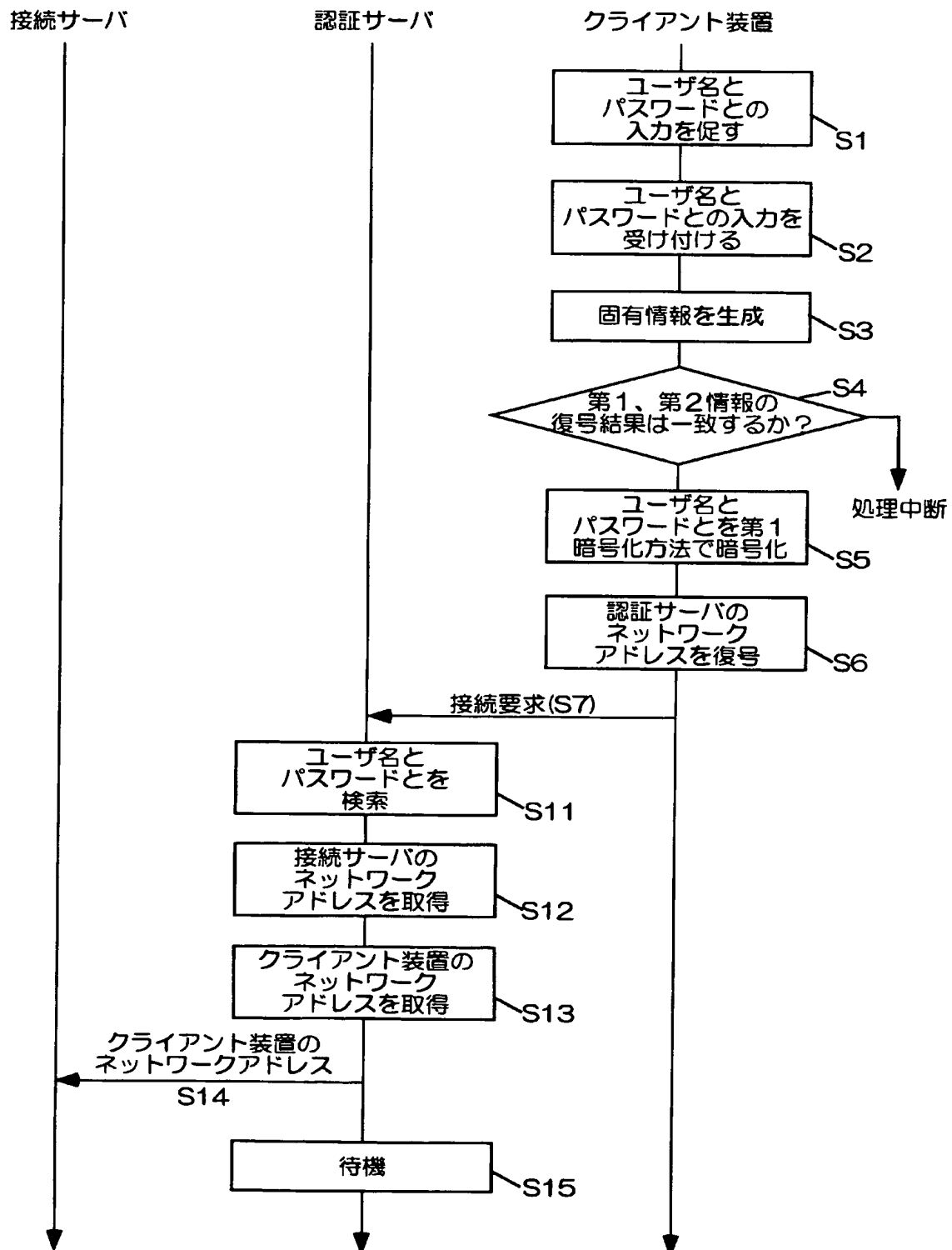
【書類名】 図面  
【図 1】



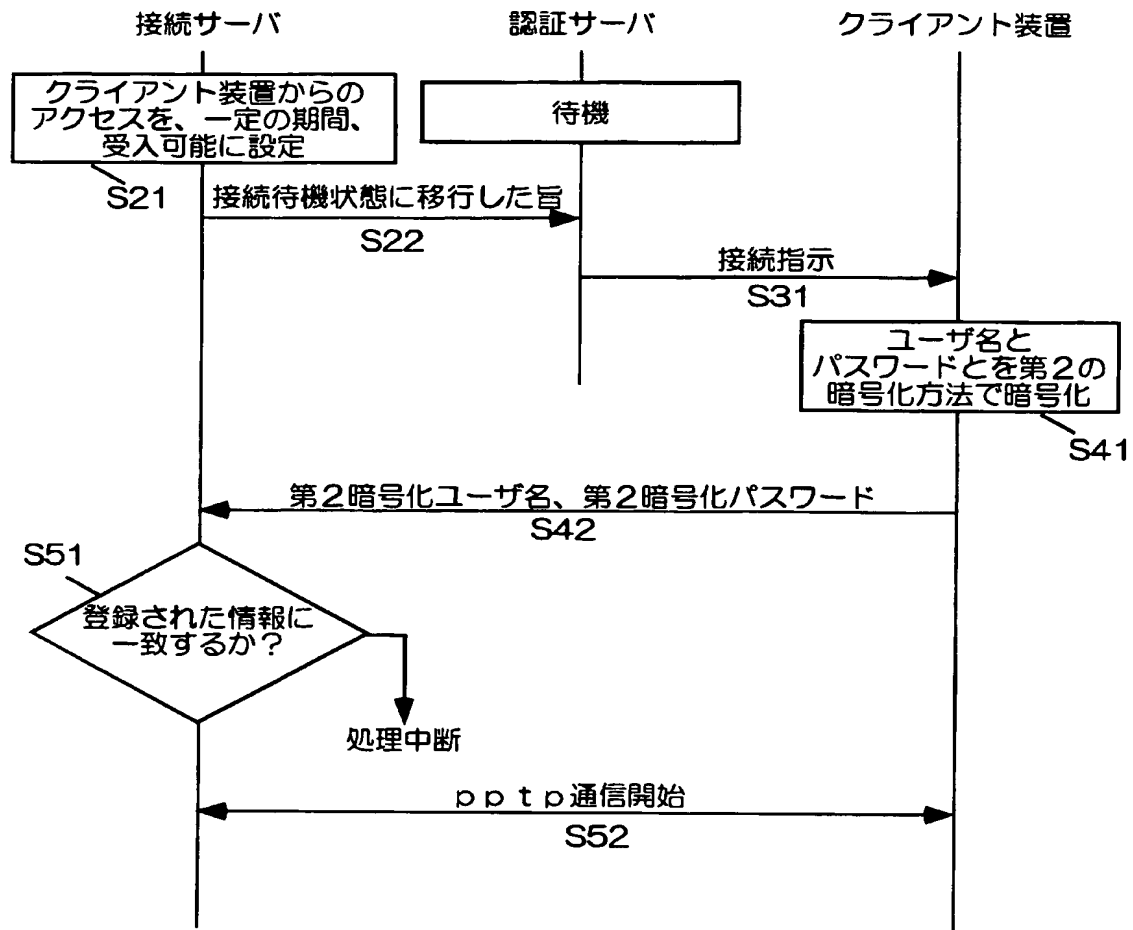
【図 2】

接続サーバの ネットワークアドレス	第 1 暗号化 ユーザ名	第 1 暗号化 パスワード
aaaaa	bbbb	cccc
aaaaa	dddd	eeee
ffff	gggg	hhhh
aaaaa	xxxx	yyyy
⋮	⋮	⋮

【図 3】



【図 4】





【書類名】 要約書

【要約】

【課題】 リモートアクセスにおけるセキュリティを向上できるネットワーク接続システムを提供する。

【解決手段】 クライアント装置 3 と、認証用サーバ 4 と、接続サーバ 1 1 とを含むネットワーク接続システムであって、認証用サーバ 4 がクライアント装置 3 のユーザを認証し、接続サーバ 1 1 にクライアント装置 3 のネットワークアドレスを通知する。接続サーバ 1 1 から接続待機状態に移行した旨を表す情報を受信すると、当該ネットワークアドレスをクライアント装置 3 に対して送出し、クライアント装置 3 が当該ネットワークアドレスに暗号化したユーザ名とパスワードとを送信して、接続サーバ 1 1 が、当該暗号化されたユーザ名及びパスワードを用いた認証を行う。

【選択図】 図 1

## 認定・付加情報

特許出願の番号	特願 2004-035481
受付番号	50400227236
書類名	特許願
担当官	第八担当上席 0097
作成日	平成 16 年 2 月 17 日

## &lt; 認定情報・付加情報 &gt;

## 【特許出願人】

【識別番号】	000005496
【住所又は居所】	東京都港区赤坂二丁目 17 番 22 号
【氏名又は名称】	富士ゼロックス株式会社

## 【代理人】

申請人	
【識別番号】	110000154
【住所又は居所】	東京都新宿区新宿二丁目 4 番 16 号 栄幸ビル 9 階
【氏名又は名称】	特許業務法人はるか国際特許事務所

特願 2 0 0 4 - 0 3 5 4 8 1

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 5 4 9 6 ]

1. 変更年月日	1 9 9 6 年 5 月 2 9 日
[変更理由]	住所変更
住 所	東京都港区赤坂二丁目 1 7 番 2 2 号
氏 名	富士ゼロックス株式会社